«25 октября 2007 г в Москве, в отеле «Марко Поло Пресня» прошёл четвёртый интеллектуальный конгресс, организатором которого выступил Евразийский Союз Молодежи. Мероприятие проходило в закрытом режиме, а слушателями подрастающей элиты стали представители МИДа, посольств, аналитических и исследовательских центров, Генштаба РФ, спецслужб и др. силовых ведомств» (Сообщение о конференции, опубликованное на сайте http://www.rossia3.ru/mer/4kongress_nets).

Один из руководителей конференции — лидер международного Евразийского движения А.Г.Дугин — опубликовал свой доклад в "Литературной газете" № 51, 2007 г. (приведён в Приложении). Поскольку его содержание, на наш взгляд, неадекватно реально происходящим процессам, то было принято решение опубликовать в интернете и тезисы выступления представителя ВП СССР В.М.Зазнобина, — "Информационная безопасность в режиме «сетевой войны»", приглашённого на конференцию в качестве консультанта-эксперта МИД РФ. Тезисы выступления В.М.Зазнобина и наш комментарий к докладу А.Г.Дугина предлагаются вниманию читателя.

Информационная безопасность в режиме «сетевой войны»

Рассмотрение вынесенной на конференцию проблематики наиболее эффективно вести в терминологии Достаточно общей (в смысле универсальности применения) теории управления (ДОТУ), поскольку всякий процесс может быть интерпретирован как процесс управления либо самоуправления. Здесь необходимо подчеркнуть, что ДОТУ и «кибернетика» в её исторически сложившемся виде это — содержательно разные вещи.

При взгляде с позиций Достаточно общей теории управления информационная безопасность это — устойчивое течение процесса управления объектом (самоуправления объекта), в пределах допустимых отклонений от идеального предписанного режима, в условиях целенаправленных сторонних или внутренних попыток вывести управляемый объект из предписанного режима.

Таким образом, термин «информационная безопасность» всегда связана с конкретным объектом управления, находящимся в определенных условиях (среде). Но кроме того он относится к полной функции управления, представляющей собой совокупность разнокачественных действий, осуществляемых в процессе управления, начиная от идентификации факторов, требующих управленческого вмешательства и формирования целей управления, и кончая ликвидацией управленческих структур, выполнивших свое предназначение.

Это общее в термине «информационная безопасность» по отношению к информационной безопасности как самого мелкого и незначительного дела, так и информационной безопасности человечества в целом.

При более широком взгляде информационная безопасность в определённом выше смысле — средство обеспечения безопасности по всем параметрам всякого культурно своеобразного общества в границах государства, и далее — человечества в целом в глобальном историческом и глобальном эволюционном процессе биосферы Земли. Вне разрешения этой проблематики права человека не могут быть гарантированы.

Последнее по существу означает, что информационная безопасность в этих аспектах носит двухуровневый характер, обеспечиваемый:

- избранием концепции глобализации (в смысле построения единой культуры человечества, интегрирующей в себя все национально-своеобразные культуры в их лучших проявлениях), гарантирующей разрешение глобального биосферно-экологического и социального кризиса и дальнейшее развитие человечества и каждого из составляющих его народов без социальных конфликтов в условиях здоровых биоценозов планеты во всех регионах обитания и хозяйственной деятельности;
- качеством управления по избранной концепции глобализации и приведением в соответствии с нею внутренней и внешней политики государств планеты.

Одно из наиболее широких определений, которое можно дать термину «сетевая война», — война, в которой невозможно однозначное определение противника и линии фронта, разделяющей территории, подконтрольные воюющим сторонам. Это — более ёмкое определение, нежели предлагаемое многими понимание сетевых войн, как войн исключительно «конспирологического характера», что подразумевает действия в обществе противника неких тайных организаций либо организаций с «двойным» и «тройным дном». Но для того, чтобы такое определение не было бессодержательно-пустым и могло бы быть продуктивным в деле обеспечения безопасности общества и развития человечества, необходимо владеть понятийным аппаратом Достаточно общей теории управления.

В частности надо понимать, что средства ведения войны (обобщённое оружие) являются в то же самое время и средствами управления. Если под оружием понимать любые средства борьбы противостоящих общественных групп, в том числе и государств, и расставить его приоритеты в порядке убывания губительности, мы получим следующее.

ИНФОРМАЦИОННОЕ ОРУЖИЕ: 1. Информация философского, мировоззренческого характера — методология познания, поскольку именно философия представляет собой своего рода «камертон», по которому настраиваются все прикладные науки. 2. Информация летописного, исторического, хронологического характера каждой отрасли знания. 3. Информация прикладного фактологического характера каждой отрасли знания (идеология, технология и т.п.)

МАТЕРИАЛЬНОЕ ОРУЖИЕ: 4. Экономика и международная торговля. Борьба за мировые деньги. 5. Угроза применения оружия массового поражения (не уничтожения, а поражения!), наиболее разрушительными из которого являются алкоголь, прочие наркотики, а подчас и общеупотребительные в жизни вещества, разрушающие психику и генетику человека. 6. Прочие виды оружия, главным образом силового воздействия на противника и его собственность, что и понимается большинством в качестве средств ведения войны, а средства более высоких приоритетов в таковом качестве не рассматриваются.

Применение обобщённых средств управления / оружия реально протекает на основе трёх способов управления:

- **Структурное управление**, основанное на предварительном создании структур с однозначно определённой функциональной нагрузкой элементов в архитектуре структуры и компетенцией входящих в её состав управленцев и прочего персонала.
- **Бесструктурное управление**, основанное на безадресном распространении в среде информации, откликаясь на которую среда

сама из своих элементов порождает множество функционально целесообразных структур. По существу бесструктурное управление представляет собой управление статистикой откликов среды на прохождение в ней информации.

- **Управление на основе виртуальных структур.** Оно на всяком иерархическом уровне в организации среды, проводящей информацию, представляет собой выражение иерархически высшего по отношению к нему управления, в ходе которого структуры заблаговременно развёртываются в среде, проводящей информацию, но они не видны с того иерархического уровня, в котором развёрнуты. В силу этого управление на основе виртуальных структур с этого уровня среды может восприниматься как «спонтанные процессы», которые носят неуправляемый характер.

Сетевая война — не битва одиночек. Поэтому субъект, претендующий на реализацию своих целей в режиме «сетевых войн» и не владеющий всеми названными выше средствами, обречён на поражение. Это неизбежное следствие того, что даже если он сам бессознательно эффективно владеет всем названным, то в силу коллективного характера деятельности общества в режиме «сетевых войн», не освоив понятийный аппарат ДОТУ и не распространив его в обществе, он не состоянии выстроить долговременную стратегию ведения такой войны и организовать общество на победу в такой войне. Это сродни тому, как циклоп Полифем проиграл «коварному Никто», под каким псевдонимом выступал хитроумный Одиссей.

24 октября
2007 г.

Комментарий к докладу А.Г.Дугина

После того, как был прослушан основной доклад А.Г.Дугина на конференции «Информационная безопасность и сетевые войны», а также выступления многочисленных гостей, в том числе зарубежных, стало ясно, что термин «Сетевые войны», введённый интеллектуалами из состава “элит” США и разрекламированный А.Г.Дугиным — всего лишь один из аспектов ведения (холодной) информационной войны, которая идёт столько же, сколько существует человечество. Об этом на конференции было прямо сказано в выступлении представителя ВП СССР. Действительно, только в теории «информационных войн», разработанной более 20 лет назад ещё в бытность СССР авторским коллективом ВП СССР чётко разграничены приоритеты обобщённых средств управления / оружия, опираясь на которые можно выявлять алгоритмы ведения так называемых «сетевых войн» и разрабатывать меры противодействия им на всех приоритетах обобщённых средств управления / оружия, включая идеологический и экономический. Другими словами, невозможна никакая «сетевая война» в толпо-“элитарном” обществе индивидуалистов, отрицающих объективность интересов общественного развития, если её операции своевременно и в достаточной мере не профинансированы.

В то же время, с точки зрения первого приоритета обобщённых средств управления (познавательно-методологического) подмена адекватного термина на неадекватный — в отношении всякого объективного явления и образных представлений о нём — есть акт агрессии со стороны противника, ведущего информационную войну.

Чтобы не быть голословными, покажем это на конкретном примере, благо доклад А.Г.Дугина, прочитанный на конференции «Информационная безопасность и сетевые войны» почти полностью опубликован в «Литературной газете» (№ 51, 2007 г. — вынесена в Приложение к настоящей записке). Предлагаем всем, кто знаком с ДОТУ и приоритетами обобщённых средств управления по материалам ВП СССР, поменять в этой статье термин «сетевые войны» на термин — «информационные войны», после чего всё встанет на место.

Что же получается? — Как это не покажется парадоксальным, но главный борец с «сетевыми войнами» предстаёт как пустобрёх и агент влияния в России заокеанских разработчиков теории и практики «сетевых войн».

Для чего это делается?

- С одной стороны, — им самим, чтобы доказать свою незаменимость в политическом истеблишменте России в качестве консультанта по неведомым и непонятным для бюрократов «сетевым войнам»,
- а с другой стороны — его кукловодами, чтобы парализовать политическую волю руководства России: ведь они всё равно не знают, что такое «сетевые войны», но термин звучит завораживающе-парализующе для тех, кто не знает ДОТУ и не в состоянии на её основе интерпретировать поток событий жизни.

24 декабря 2007 г.
Внутренний Предиктор СССР

ПРИЛОЖЕНИЕ

Новейшая история
Сеть для России
КОНСПИРОЛОГИЯ
Наше государство — главная цель в сетевой войне

Что есть Путин для России? Путин — это стремление утвердить заново суверенитет России. Путин — это не суверенная демократия, Путин — это просто суверенитет, демократия же — это в нагрузку или для внешнего пользования. Может быть, Путин действительно искренне верит в демократию. Но это неважно, т.к. много кто искренне верит в демократию, но они из-за этого Путиными не становятся. Чаще всего искренне верующие в демократию люди становятся чем-то противоположным Путину, то есть оранжевыми, врагами России и русского народа.

То, что в Путине не суверенитет России, — это второстепенно и незначимо, это, как говорят философы, «акциденции». Смысл Путина в том, чтобы укрепить суверенитет России. В этом же и смысл преемственности. Будет укрепляться и отстаиваться в условиях глобализации суверенитет России — будет преемственность, не будет — не будет преемственности. Поэтому неважно — кто преемник, неважно, как Путин решит даже собственную судьбу после марта 2008 года. Всё это второстепенно перед вопросом: будет ли охраняться и укрепляться суверенитет России или он ослабнет? В этом и заключается «план Путина».

Каковы же угрозы курсу на суверенитет, кто является «врагом» для «плана Путина»? В сегодняшней выборной ситуации серьёзных угроз не существует. Парламент с нормальной, вменяемой левой, коммунистической оппозицией является не угрозой для стабильности России, а наоборот — залогом полной благостности в партийно-политическом пространстве. Однако существуют вызовы и угрозы куда более серьёзные. Дело в том, что США стремительно меняют манеру и методологию взаимодействия с другими государствами, оттачивая технологии так называемых сетевых войн.

Сетевые войны ведутся преимущественно в информационной сфере и основаны на использовании «эффекта резонанса», когда внешние операторы манипулируют самыми разнообразными, не связанными между собой идеологическими, общественными, гражданскими, экономическими, этнологическими, миграционными процессами для достижения конкретных целей. Главная же задача здесь — десуверенизация. Однако сетевая война ведётся американцами, по их собственному признанию, не только против своих противников, но и против своих союзников и нейтральных сил. Поскольку в нынешней глобальной системе США не допускают наличия никакой иной субъектности, помимо своей собственной. То есть существование суверенности не предусмотрено даже для союзников, которые тоже подвергаются десуверенизации, как и противники.

Таким образом, мы имеем дело с новой моделью взаимоотношения стран (и в первую очередь России) с США, которая не сводится к обычной логике: друзья — враги, конкуренция — партнёрство, противостояние — сотрудничество. Логика сетевых войн лежит в другой плоскости. И, к сожалению, наш президент и наше руководство принципиально не готовы осознать эту ситуацию. Они иначе воспитывались, они совершенно не учитывают ни постмодерн, ни сеть — и в этом главная угроза суверенитету России.

Власть в целом и Путин лично сегодня беззащитны перед сетевыми вызовами со стороны США и не готовы адекватно реагировать — в силу других исторических традиций, а также из-за огромного количества технических и хозяйственных проблем, которые власть вынуждена решать. Но именно глобальная сетевая война сегодня является главным содержанием мировой политики. Для такой войны не существует государственных границ, для неё нет преград, нет зон влияния национальных администраций. И если прямое вмешательство внешних сил можно пресечь, как это сейчас делает Путин, то множество, тысячи сетевых каналов осуществления внешнего влияния ни государством, ни даже самыми бдительными спецслужбами не фиксируются, не идентифицируются как таковые. Потому что технологии сетевой войны являются очень тонкими и оперируют с тем, что у любого чиновника, даже спецслужбиста, протекает сквозь пальцы...

Необходимо также понять, что основы инфраструктуры сетевой войны в России американцы заложили в 80-е и особенно в 90-е годы. Наше общество сплошь пронизано различными сетями, которые не идентифицируются ни как враждебные, ни как подрывные, не являются прямой агентурой западных спецслужб, не получают деньги за «продажу Родины», но при этом они координируются внешними центрами с помощью особых технологий. Тот факт, что существует активный внешний игрок, имеющий мощный сетевой инструментарий внутри Российской Федерации, великолепно отлаженные в онлайн-режиме системы сетевого влияния, и составляет фундаментальную угрозу для Путина и его курса.

Суверенитет нашего государства постоянно находится под угрозой системных сетевых атак, которые используют любые «дыры» в легальности российского законодательства. В частности, фатальную для Путина невозможность конституционного третьего срока, а также разделение властей, отсутствие национальной идеи, депрессивное интеллектуальное состояние элиты, одним словом — любые объективные причины. Американцы используют также множество сетей, естественных и искусственных, которые пронизывают наше общество на всех уровнях и с помощью новейших информационных технологий, пользуясь объективными проблемами в нашей стране. И всегда будут играть на десуверенизацию, используя для этого все подворачивающиеся под руку возможности. И эта угроза нарастает.

Чем больше Путин будет настаивать на суверенитете — как он это делает сейчас, пусть грубовато, но зато эффективно и действенно, — тем больше будут нарастать риски. Постепенно в этой сетевой войне будут задействованы очень сложные, многомерные, фундаментальные сетевые стратегии, к которым наша власть не готова. И здесь американцы будут использовать не только откровенную либеральную пятую колонну, но и национализм, социальную проблематику, экспертные сети, в том числе — научный мониторинг, молодёжные движения, интеллектуалов. По сути дела, гражданское общество, которое мы строим, является максимально удобной платформой для ведения сетевой войны, поскольку в техническом смысле оно и есть оптимальное пространство для эффективного ведения сетевых войн. Институты гражданского общества не подлежат, как правило, жёсткой юрисдикции и плотному административному контролю и соответственно в сетевых условиях становятся наиболее эффективной и не контролируемой государством средой десуверенизации. Таким образом, гражданское общество, различные неправительственные организации, фонды, движения, экспертные сети, гранты, научные сообщества, группы

людей по интересам, институты исследования этнических проблем — всё вместе это, включая, кстати, и радикальные, и интеллектуальные центры, будет задействовано американцами в ближайшее время.

Это очень серьёзный вызов, который в таком качестве не встречался ранее в нашей истории. Мы прожили эпохи войн государств против государств, мы знаем идеологическую борьбу двух мировых лагерей — капиталистического и социалистического. И если в модели «государство на государство» мы способны выигрывать, то идеологическую борьбу с Западом мы проиграли, причём дважды — один раз в 1917 году, позволив опрокинуть царский режим, который был основан на вполне определённой православно-монархической русской идеологии, а потом — советский режим в 1991 году, где русский, а также мессианско-монархический фактор выступал косвенно. И в обоих случаях огромную роль сыграли внешние сети: от этнических групп до религиозных сект и политических заговорщиков, в свою очередь, густо приправленные прямыми шпионами и коррумпированными представителями собственных спецслужб.

Россия, подчас неуязвимая для прямого вторжения, способна вести и отстаивать свой суверенитет в горячих войнах, хотя и большими жертвами. Но для тонкого идеологического сетевого проникновения она весьма уязвима. То, что происходило с Россией в 90-е, американцы — в значительной степени оправданно — рассматривали как оккупацию побеждённой и сломленной вражеской державы. Мы проиграли в холодной войне и были оккупированы. В лице Ельцина и его команды, которая работала на них в то время (олигархи, реформаторы, «семья», говорливые эксперты и политтехнологи, на сто ладов воспевавшие ценности «демократии» и «свободы»), мы имели колониальную администрацию, осуществлявшую в стране внешнее управление, как в Японии или в Германии после 45-го года. От краха СССР и последующей оккупации и разгрома 90-х до сих пор поднимается кровавый пар... С Путиным мы наконец стали выползать из режима этой оккупации, стали восстанавливать суверенитет. Но надо учитывать: система оккупационной власти — Ельцин, олигархи, «семья», коррумпированные кланы, предательская интеллигенция и компрадорская буржуазия — внедрила внешние сети ещё глубже, на несколько уровней. Сегодня эти сети пропитывают современное российское общество.

Складывается впечатление, что Путин и его ближайшее окружение интеллектуально, исторически, идеологически не готовы к полноценному ведению этой сетевой войны. Субъективно, морально, этически, по совести — Путин за суверенитет. Он и есть гарант суверенитета. Но отстаивать суверенитет и продолжать оставаться гарантом суверенитета в новых условиях, которые становятся всё более и более сложными для России в условиях эскалации сетевых войн, Путину будет всё труднее и труднее. Пока что не видно каких-то признаков того, что власть всерьёз озабочена эффективным ведением сетевой войны. Многие и не подозревают, что это такое. Термин «сетевая война» сегодня звучит как нечто экстравагантное.

Если мы не мыслим в категориях сетевой войны, значит, мы просто живём в неадекватном смысловом пространстве, не понимаем, что происходит и будет происходить с нами, не понимаем, какие вызовы и угрозы существуют в отношении преемственности курса, в отношении России и Путина. Многие известные политологи и эксперты спрашивают: что такое «сетевая война» и с чего вы взяли, что она против нас ведётся? Это значит, что ещё некоторое время уйдёт на доказательство её наличия и того, что она ведётся против нас в данный момент. Страшно смотреть на

то, как медленно соображают наша власть и наше общество, и, к сожалению, много времени уйдёт на то, чтобы доказать с приведением фактов, примеров, цифр, графиков, что эта сетевая война ведётся против нас — на уничтожение. И только поняв, признав и осознав это, можно будет говорить о том, как её эффективнее вести с нашей стороны.

Существует сетевой миф о том, что война якобы ведётся между Америкой и исламским фундаментализмом. И, увы, этот миф имеет подтверждение: мы сетевую войну не ведём. Её ведут против нас, а мы об этом и не подозреваем... Мы ещё не стали субъектом ведения этой сетевой войны. Мы — её объект, жертвенное животное, которое готовят на заклание. Животное тоже чувствует приближение своего конца, оно мычит, отбивается, не хочет идти на убой, у него есть интуиция смерти. У нас тоже есть интуиция, и мы чувствуем, что нам что-то угрожает. Но между интуицией барана и волей к суверенности свободного и разумного мыслящего существа есть огромная разница...

Сам миф о том, что есть только Запад, который борется с международным терроризмом, и что надо быть на стороне Запада в этой борьбе, является одной из форм эффективного ведения сетевых войн. Даже одна эта идея уже может быть элементом подрывной стратегии — настолько тонкие вещи определяют эту войну. Надо понять: если мы хотим выжить, сохранить свой суверенитет, нам необходимо осознанно включиться в эту сетевую войну — против США и их мировых сетей — внешних и внутренних, необходимо уже сейчас начать вести её самым активным образом. Не только обороняться, но и наступать. Мы должны усвоить правила её ведения, выяснить, какие инструменты она использует. Пока что мы отвечаем чаще всего интуитивно.

К нам завозят различные НПО, экспертные сети, такие фонды, как «Евразия» и «Новая Евразия», финансируемые ЦРУ, нам подбрасывают «говорящие камни», используют Касьяновых и Каспаровых — с этим мы как-то справляемся. Интуитивно подражая противнику, в ответ мы пытаемся создать свои НПО. Может быть, это и правильно, но явно наши НПО, судя по тому, как распределяется поддержка среди них, кому выдаются гранты, какие задачи им ставят, являются, увы, просто формой освоения бюджета. Мы имитируем деятельность врага. Это будто компьютер, искусно вытесанный из камня или из дерева, поделка русского гениального Левши XXI века. Но дело в том, что смысл компьютера не в его внешней форме, мы же лишь подражаем, создавая его идеальные каменные аналоги. Увы, именно так мы реагируем на ведение против нас сетевой войны. Эта реакция является в лучшем случае пародийной, симуляционной либо её вообще нет.

Власти необходимо совершить колоссальное интеллектуальное усилие, поскольку сетевые войны, их практика, их стратегия, их тактика, их методология основаны на серьёзном философском понимании процессов, протекающих в современном мире. Мы живём обрывочными фрагментарными представлениями. И в таких условиях нами очень легко манипулировать. Мы не ведём сетевой войны, у нас нет своей позиции даже по ближнему зарубежью. Нет позиции по Украине, Грузии, Молдове, Азербайджану... Мы только радуемся, когда оранжевые вдруг переругались, или злорадствуем, что американцы меняют антироссийского Саакашвили на ещё более антироссийского Окруашвили, чтобы быстрее натравить Грузию на Южную Осетию и Абхазию и втянуть Россию в новый конфликт. Мы радостно освещаем внутренние проблемы Грузии, хотя сами палец о палец не ударили для того, чтобы создать Саакашвили по-

настоящему серьёзные проблемы и предложить по-настоящему серьёзную — пророссийскую, евразийскую — альтернативу грузинской политике. Мы можем только наслаждаться промахами и провалами наших противников. Мы только совсем недавно смутно начали осознавать, что Америка — наш противник, но и это уже хорошо. Однако ни инструментария, ни опыта эффективного противодействия опасным и очень эффективным сетевым стратегиям США у нас нет и близко.

Путин опутан сетями. Сети проникли в российскую власть с 90-х годов. И если прямых сторонников десуверенизации России оттуда постепенно устранили, а те, которые остались, не играют большой политической роли, то атлантистские сети всё равно остались рядом с властью. Большое количество подобных людей сейчас находится в Общественной палате РФ. Может быть, они ничего и не решают и именно так власть хочет их «перекодировать», но это опасно. От своих агентов в среде диссидентуры кураторы из КГБ СССР настолько заразились западными мифами, что провалили страну и режим, которым присягали на верность, и это тоже сетевые технологии. В 90-е годы американские стратеги ловко и тонко проникли в структуры силовиков, создав там очаги влияния. И даже за патриотическим настроем некоторых силовых группировок в окружении президента легко угадываются те же самые инструменты, те же самые нити, те же самые сети. Казалось бы, одни — сторонники либерализма, откровенные западники, и с ними всё понятно, но другие-то — наоборот, националисты, патриоты, противники Запада. Вот только манипулируют ими одни и те же операторы из Вашингтона. Силовикам в отличие от либералов и правозащитников никто напрямую не говорит: «Давайте десуверенизируем Россию». Это говорит только Каспаров или гламурный, выживший из ума Лимонов, которых уже никто не слушает. С силовиками же всё тоньше. Ими манипулируют через национализм: неявно, потакая провокациям в духе «Русского марша», некоторые силовики также подыгрывают Западу, который прекрасно понимает, что русский национализм является таким же эффективным сетевым оружием в развале России, как и национализм малых этносов, — только ещё более действенным и разрушительным...

Есть множество людей, которых слушают, которые выступают на телевидении, являются консультантами президента, организаторами серьёзных экспертных сетей, представляя собой интеллектуальный оплот путинской власти, но при этом огромный процент из них представляют собой сегменты американской сети влияния. Они действуют более тонко, но направлены прямо или косвенно на десуверенизацию России. Пусть скажут, что это напоминает охоту на ведьм, однако, как любит повторять один кремлёвский высокопоставленный чиновник, «если у вас паранойя, это ещё не значит, что вас никто не преследует».

Нынешняя сетевая пятая колонна не такая простая и прямолинейная. Нам подчас хотят изобразить, что всё дело только в СПС или в «маршах несогласных». Но это — самая откровенная вершина айсберга. Более того, это — ложная цель. Самые серьёзные сети влияния, направленные на десуверенизацию России, находятся среди тех, кто близок Путину, кто его поддерживает и с ним работает, кто предопределяет и в значительной степени влияет на выработку его стратегии. Вот где надо искать настоящий заговор. Ведь заговор — это просто устарелое «архаическое» название для обозначения того явления, которое сегодня открыто принято называть «сетевой войной».

Александр Дугин